26. (New) The method of claim 25 wherein a first secure bitstream will configure properly user-configurable logic of the first plurality of programmable integrated circuits, but not the second plurality of programmable integrated circuits.

27. (New) The method of claim 25 further comprising:

loading an unencrypted bitstream into one of the first plurality of programmable integrated circuits to generate a secure bitstream using the first secret key.

28. (New) The method of claim 25 wherein the first plurality of programmable integrated circuits with the first secret key are assigned to a first geographic area and the second plurality of programmable integrated circuits with the second secret key are assigned to a second geographic area.

29. (New) The method of claim 25 wherein the first plurality of programmable integrated circuits with the first secret key are fabricated in a first time period and the second plurality of programmable integrated circuits with the second secret key are fabricated in a second time period, different from the first time period.

30. (New) The method of claim 25 wherein only one mask differs between the first and second mask sets.

31. (New) The method of claim 25 wherein the first plurality of programmable integrated circuits with the first secret key are assigned to a first customer and the second plurality of programmable integrated circuits with the second secret key are assigned to a second customer.

32. (New) The method of claim 29 wherein the first time period is about the same duration as the second time period.

33. (New) The method of claim 29 wherein the first time period is a different duration from the second time period.

34. (New) The method of claim 30 wherein the one mask is a contact mask.

35. (New) The method of claim 25 wherein there are random differences between artwork of the first and second plurality of programmable integrated circuits in addition to the different embedded secret keys.

36. (New) The method of claim 25 wherein the first and second secret keys are presented on wires of respective plurality of programmable integrated circuits for only a limited duration.

37. (New) The method of claim 25 wherein the first secret key is embedded by setting an initial state of a random selection of memory cells in a device configuration memory of the programmable integrated circuit.

38. (New) The method of claim 37 further comprising:

extracting the first secret key by using a CRC algorithm to compute a checksum of the initial state of the device configuration memory.

a1

39. (New) The method of claim 25 further comprising:

loading an unencrypted bitstream into one of the first plurality of programmable integrated circuits to generate a secure bitstream based on the first secret key and an on-chip generated random number.

40. (New) The method of claim 25 further comprising:

loading an unencrypted bitstream into one of the first plurality of programmable integrated circuits to generate a secure bitstream based on the first secret key and an on-chip generated random number, wherein the secure bitstream inlcudes a message authentication code.

41. (New) The method of claim 25 further comprising:

downloading a secure programmable integrated circuit bitstream through a network; and

configuring one of the first plurality of programmable integrated circuits using the secure programmable integrated circuit bitstream by decoding the secure programmable integrated circuit bitstream using the first secret key.